IETF 115, London
OAuth WG
November 2022

Atul Tulshibagwale
CTO, SGNL
Twitter: @zirotrust
LinkedIn: @tulshi

Fine-grained Transactional Authorization (FTA)

Workgroup Update

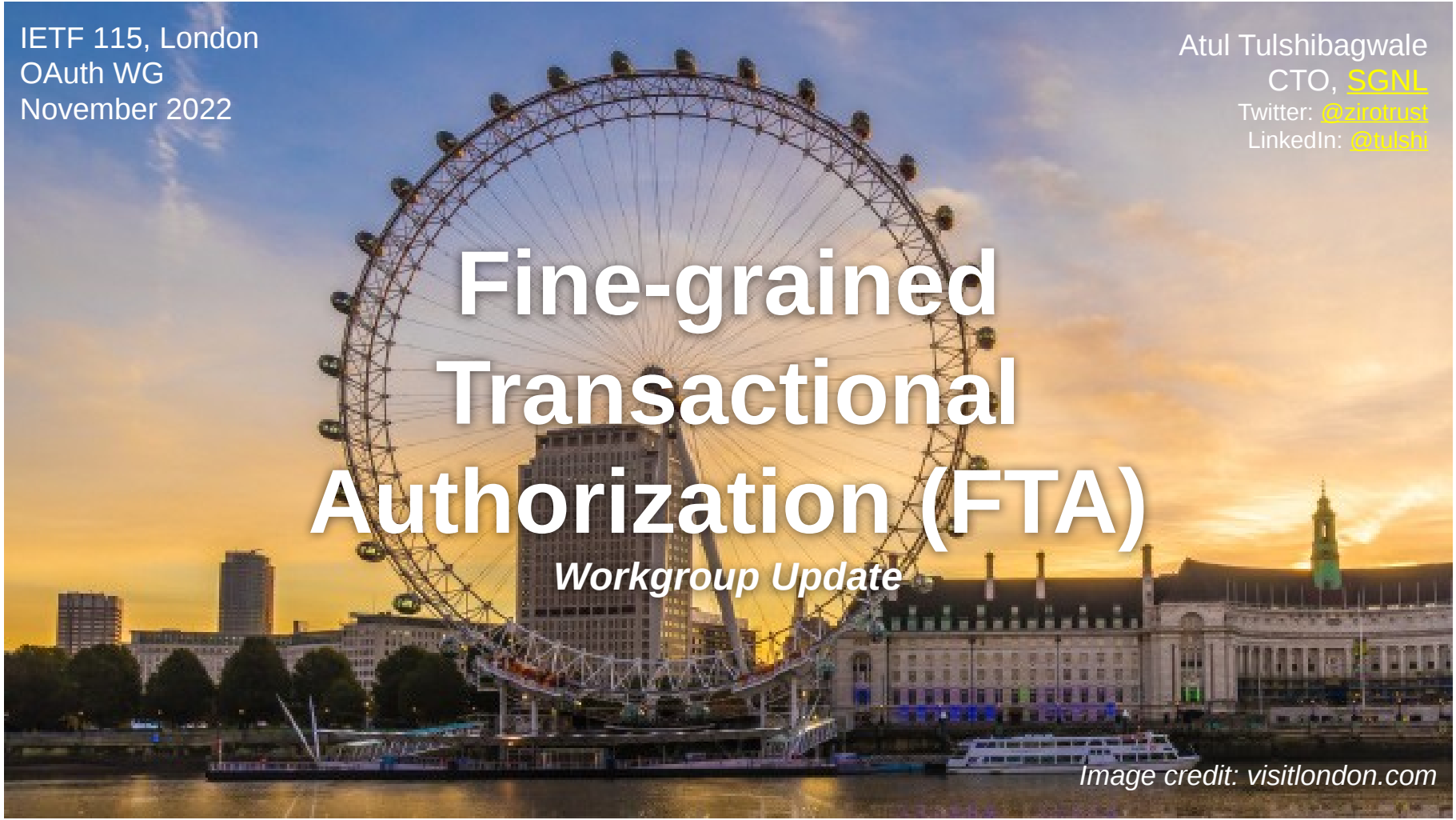


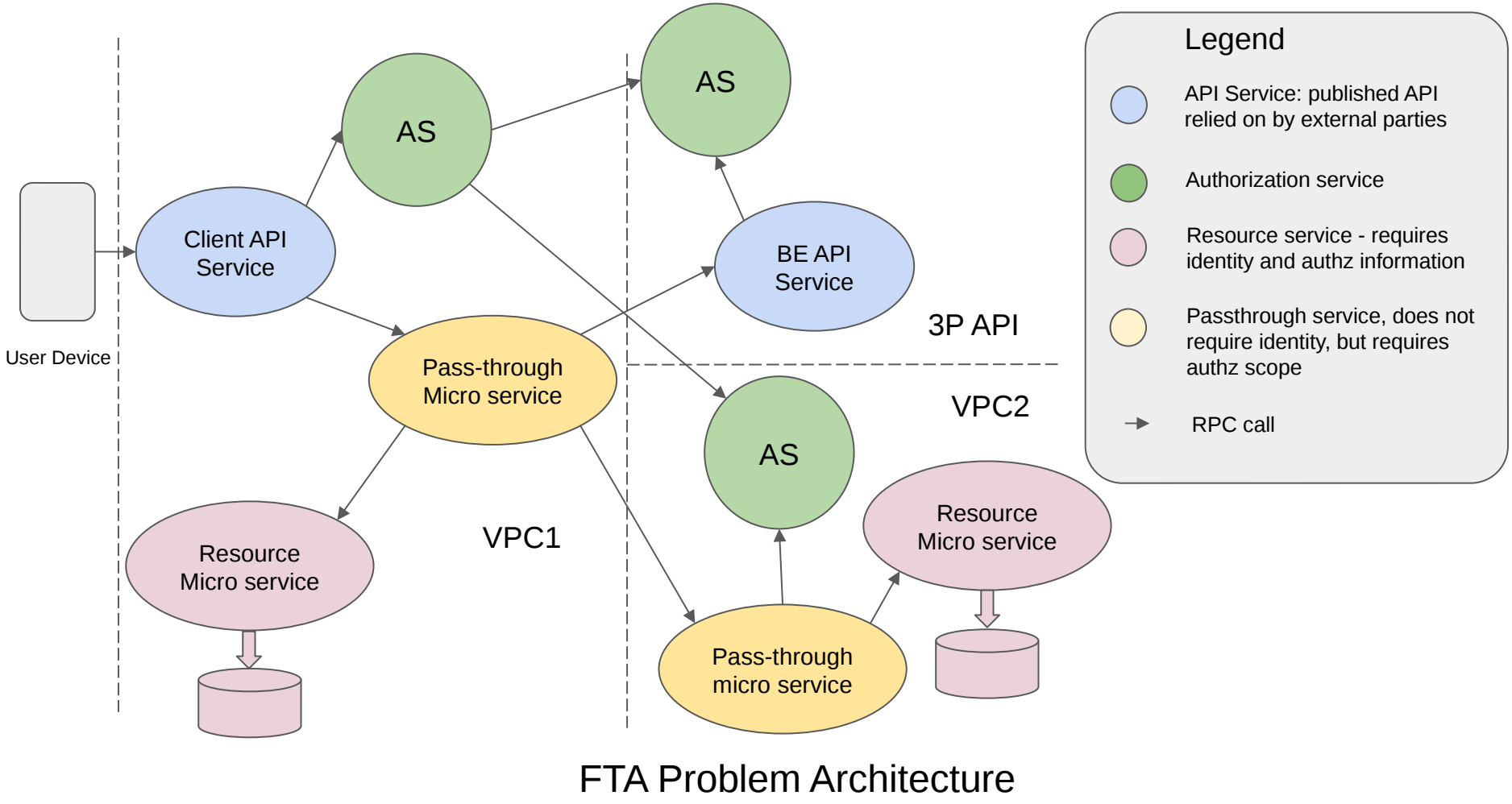
Image credit: visitlondon.com

FTA Motivation

- Securing authorization and identity information in microservice communication
- Defense against software supply chain and privileged user compromise attacks
- Needs open-standard to work across multiple cloud platforms and multiple on-premise technologies

Background

- Prior Work
  - Netflix blog - Edge Authentication, protobuf “Passport” tokens, HMAC signatures
  - Athenz - Verizon supported open-source for “AuthNZ”; Centralized and decentralized authz
- Related presentations
  - George Fletcher at Identiverse 2020 - short-lived Transaction Tokens, JWT based
  - Rifaat Shekh-Yusef at IETF 114 - OAuth multi-subject tokens
  - Dr. Kelley W. Burgin at IETF 114 - OAuth token chaining
  - Atul Tulshibagwale at IETF 114 - Describes the problem architecture



FTA Problem Architecture

Background (Continued)

- Charter discussion
  - Group workshop on 9/21
  - Group call on 10/14
  - Attendees include AWS, Capital One, Google, Microsoft, MITRE, NSA and SGNL

- Charter document proposed by SGNL, Okta, NSA, Microsoft and AWS
  - Other attendees may add themselves as proposers later
  - Available here:

Charter : Terms Defined

- Interactive and Batch Invocations
- Synchronous and Asynchronous Invocations
- Trust Boundaries
- RPCs
- Call Chain

Charter: Purpose

To enable services within the same trust boundary and across trust boundaries to securely and interoperably convey authentication, least-privilege, fine-grained authorization, call chain, and call context information in communication between independent services.

Charter: Scope

- A framework for communicating identities across trust boundaries (to the extent required to communicate authorization information)

- A mechanism for services to securely communicate the identity and authorization information about communication between services

Identity and AuthZ Information

- Preserve Identity of the initiating principal
- Service identity of the calling service
- Service identities of participants in the call chain
- Authorization scope defined by the caller
- Authorization scope defined previously called services in the call chain
- Argument context defined by the initiating principal
- Argument context defined anywhere in the call chain

Charter: Out of Scope

- Defining a naming convention for identities
- User or robotic principal authentication
- Policy framework or language

Charter: Proposed Deliverables

- A specification that defines how identities may be communicated across trust boundaries

- A specification that defines how information (defined in the “Scope” section) relating to an RPC is conveyed between services that reside either in the same trust boundary or across trust boundaries

Current List of Proposers

- Atul Tulshibagwale, CTO, SGNL
- Erik Gustavson, Co-founder and CPO, SGNL
- Rifaat Shekh-Yusef, Senior PM @ Okta, Chair OAuth WG @ IETF
- Michael Jenkins, Secure Protocol Standards Lead, NSA-CCSS
- Pieter Kasselman, Identity Standards Architect, Microsoft
- Dean H. Saxe, Senior Security Engineer, AWS Identity, Amazon Web Services

Areas of Discussion

- Per-trust-boundary Authorization Server
- Short-lived tokens: Lifecycle and verification
- Efficiency considerations: Latency, token bloat
- Service identities and call chain verification
- Can this extend to 3P APIs
- Delegation use cases (“on behalf of” or “acting as”)

Thank You!